UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/584,605	05/31/2000	Peter Bendel	DE9-1999-0058	2850

25259 7590 12/08/2003

IBM CORPORATION
3039 CORNWALLIS RD.
DEPT. T81 / B503, PO BOX 12195
REASEARCH TRIANGLE PARK, NC 27709

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	**PAPER NUMBER**
2131	3

DATE MAILED: 12/08/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/584,605	BENDEL ET AL.	
	Examiner	Art Unit	
	Michael R Vaughan	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 May 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 May 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claims 1-22 have been examined and are pending.

Specification

Applicant is required to update the status (pending, allowed, etc.) of all parent priority applications in the first line of the specification. The status of all citations of US filed applications in the specification should also be updated where appropriate.

Claim Objections

Claims 16, 18, 20, and 22 are objected to because of the following informalities: claims are written in independent form but do not stand on their own merits. Applicant is encouraged to amend the claims so that all of the limitations are recited in the claim and not referring back to other claims. Appropriate correction is required.

Claim Rejections - 35 USC ' 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless --

the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

Claims 1, 2, 10, 11, 14, 17,18, 20, and 21 are rejected under 35 U.S.C. 102(e) as being anticipated by Handel et al (USP 6,195,651).

As per claims 1, 16, 18, 20, and 21, Handel et al teach a method and software for controlling access to protected contents on a server, the method requiring the following components to be present:

a) a server (column 34, line 19)

b) a client (column 7, lines 60-66)

c) a reader (chip card reader) for a mobile security module (chip card) (column 34, lines 59-60)

d) a security module (chip card) having at least one protected area for storing a key (column 34, lines 59-60)

e) a data line for communications between client and server characterized by the following steps (column 7, lines 60-66):

aa) sending to the server of a request to call up protected access contents (column 34, line 35)

bb) sending from the server to the client of an authentication module to be run in the client (column 8, lines 35-57)

cc) execution of an authentication protocol for authenticating the mobile security module and, where appropriate, its holder by means of the authentication module (column 7, lines 60-67 and column 34, lines 54-65)

dd) if the authentication in step cc) was successful, addition to the request in step aa) of a session ID which was generated in the course of the communications between the authentication module and the server (column 34, lines 63-66 and see attached code on column 42, pertaining to Intention List)

ee) sending of the new request to the server application (column 34, lines 63-66)

ff) checking of the session ID in the request to see that it is recorded in the server (column 34, lines 63-66)

gg) processing of the content requested for transmission and searching of the content for further links to other protected-access contents (column 34, line 60—column 35, line 8)

hh) addition of the session ID to the links identified (column 34, line 60—column 35, line 8)

ii) sending of the content modified as in step hh) to the client (column 34, line 60—column 35, line 8).

As per claims 2 and 17, Handel et al teach that the server is a web server and the protected contents are web pages which are called up via a browser by a URL request from a client (column 7, lines 60-67).

As per claim 10, Handel et al teach that a unique identifier is used to link a user with his profile (column 32, lines 23-42). This unique identifier must be a large number to prevent others from being able to target the number. Therefore, it is inherent from the teachings of Handel et al that the number is generated from a large set so that others cannot easily guess its value.

As per claim 11, Handel et al teach that the session ID shows the user to be an authorized person for all requests within a specified session (column 32, lines 23-42).

As per claim 14, Handel et al teach that the session ID generated in step dd) is recorded in a table and in that the presence of an entry in the table is a requirement for access to all the protected-access pages (column 32, lines 23-42).

Claim Rejections - 35 USC ' 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3, 4, 6, 7, 8, and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Handel et al in view of Hopkins (USP 5,757,918).

As per claim 3, Handel et al teach that the authentication protocol is executed in the followed steps:

mm) sending of the digital signature to the server

nn) checking of the correctness of the digital signature using the security module of the server.

Handel is silent in expressly disclosing that:

jj) generation of a random number by the server application when the content requested is access-protected and the requirements for access have not been satisfied, and sending of the random number to the authentication module

kk) sending of the random number from the authentication module to the mobile security module

ll) generation in the mobile security module of a digital signature which takes account of the identity number of the mobile security module, the random number and the key of the mobile security module

Hopkins teaches:

jj) generation of a random number by the server application when the content requested is access-protected and the requirements for access have not been satisfied, and sending of the random number to the authentication module (column 9, lines 10-15)

kk) sending of the random number from the authentication module to the mobile security module (column 9, lines 15-20)

ll) generation in the mobile security module of a digital signature which takes account of the identity number of the mobile security module, the random number and the key of the mobile security module (column 10, lines 37-42).

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Hopkins within the system of Handel et al because the addition of using a random number increases the security of the authentication protocol. Hopkins authentication protocol also helps to insure that correct owner of a smart card is the one who is using the smart card. Having the random number prevents someone from trying to replay an authentication handshake. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

As per claim 4, Handel et al teach that the server application is a servlet and the client authentication module is an authentication applet (column 8, lines 35-61). It is inherent that on receipt of a URL request the servlet checks the URL request for the presence of a session ID and if there is no session ID present sends an authentication applet. Handel et al teach that whenever personal data is being accessed that one must first authenticate (column 34, lines 34-66 and column 31, line 45—column 32, line 41). Therefore, a session id or profile must first be authenticated.

Handel et al is silent in disclosing that the request contains a random number to the client. The examiner supplies the same rationale for the motivation as recited in the rejection of claim 3.

As per claim 6, Handel et al teach that the authentication applet communicates with the servlet by Internet or intranet using the TCP/IP protocol (column 7, line 60—column 8, line 20).

As per claims 7 and 8, Handel et al teach that a digital signature is generated with the use of identifying information (column 34, lines 53-66). Handel et al is silent in explicitly disclosing that the digital signature is generated by means of a symmetrical encryption algorithm such as DES or triple DES or by means of an asymmetrical encryption algorithm such as RSA, DSA, or an elliptic curve algorithm. Hopkins teaches digital signature is generated by means of a symmetrical encryption algorithm (DES) with the help of a secret key agreed between client and server, or by means of an asymmetrical encryption algorithm (RSA) with the help of a private key, the server being in possession of the public key (see column 5, lines 55-60, column 4, line 60—column

5, line 6 and column 7, lines 12-25). The use of symmetrical and asymmetrical digital signatures is well known in the art. One of ordinary skill in the art would be motivated to use either method to encrypt a digital signature as Hopkins teaches.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Hopkins within the system of Handel et al because digital signatures as used by Handel et al are known to be generated in the art by the teachings of Hopkins. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

As per claim 9, Handel et al teach that error messages are produced whenever errors are generated (column 21, lines 15-22. A failed authentication attempt is an error. Handel et al also teach one must authenticate before access is granted to privileged resources (column 34, lines 33-40). Therefore, it is inherent that Handel et al teach that if the digital signature does not agree, the servlet sends an error message to the client applet.

Claims 5, 12, 13, and 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Handel et al in view of Lin et al (USP 6,052,785).

As per claim 5, Handel et al teach that the communication between the client and server take place over a secure protocol (column 7, lines 62-63). Handel et al is silent in disclosing that the secure protocol is SSL. Lin et al teaches the use of SSL to securely communicate between a client and server (column 6, line 55—column 7, line 24).

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Lin et al within the system of Handel et al because Handel teaches the use of a secure communication protocol and SSL is a secure layer protocol. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

As per claims 12 and 13, Handel et al is silent in disclosing that the session ID, which has a period of validity, loses its validity on expiry of a fixed time or when a session is terminated by means of a log-off page. Lin et al teach that the session ID, which has a period of validity, loses its validity on expiry of a fixed time or when a session is terminated by means of a log-off page (column 6, line 60—column 7, line 24). Handel et al disclose the use of session ID in the form of profiles and personas linked to a user, which has a unique identifier for each of his/her personas, or sessions (column 32, lines 23-42). Each one of the sessions is protected and is of a secure nature. Therefore, it would have been obvious to one of ordinary skill in the art to protect them with time expirations as taught by Lin et al.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Lin et al within the system of Handel et al because the time expiration helps to prevent a thief from trying to replay an authentication attempt in order to gain access to privileged information. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

As per claim 15, Handel et al teach the storing of a session ID in a table (column 32, lines 23-42). Handel et al are silent in disclosing that the entry from the table is deleted when the validity of a session ID expires or when a session is terminated by means of a log-off page. Lin et al teach that when the validity of a session ID expires or when a session is terminated by means of a log-off page, that the entry from the table is deleted (column 6, line 60—column 7, line 24). It would be advantageous to remove a session from memory in order to prevent someone from trying to reuse another person's credentials. One skilled in the art knows the use of session ID as a temporary pass that needs to be removed once it has been used.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Lin et al within the system of Handel et al because the removing the session ID from the table in memory helps to prevent a thief from trying to replay an authentication attempt in order to gain access to privileged information. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Handel et al in view of Hopkins in view of Lin et al.

As per claim 22, all of the limitations pertaining to claims 1-15 have been rejected. Therefore the examiner sites all of the teachings and motivations used for the rejections of claims 1-15 to subsequently reject claim 22.

Remarks

No claim is allowed.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patents :

6,178,504	Fieres et al.
5,668,878	Brands
5,910,989	Naccache
6,076,108	Courts et al.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

MV
Michael R Vaughan
Examiner
Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100